PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, 12/18

A2

(11) International Publication Number: **WO 00/38392**

(43) International Publication Date: 29 June 2000 (29.06.00)

(21) International Application Number: PCT/US99/31019

(22) International Filing Date: 23 December 1999 (23.12.99)

(30) Priority Data:

60/113,734	23 December 1998 (23.12.98)	US
09/247,263	10 February 1999 (10.02.99)	US

(81) Designated States: CA, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published

Without international search report and to be republished upon receipt of that report.

(71) Applicant *(for all designated States except US)*: NORTEL NETWORKS CORPORATION [CA/CA]; World Trade Center of Montreal, 380 St. Antoine Street West, 8th Floor, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventor; and

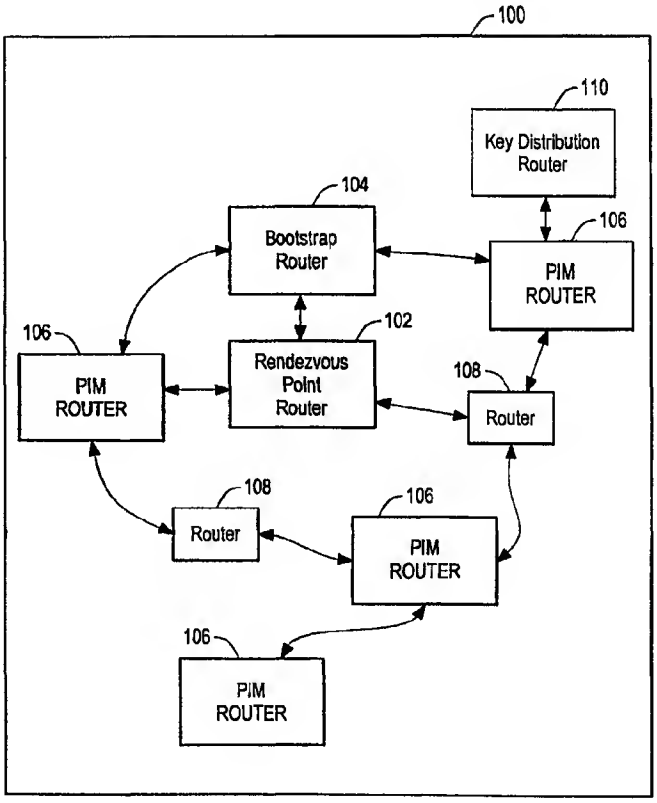
(75) Inventor/Applicant *(for US only)*: HARDJONO, Thomas [AU/US]; 10 Fessenden Road, Apt. 1, Arlington, MA 02476 (US).

(74) Agents: SUNSTEIN, Bruce, D. et al.; Bromberg & Sunstein LLP, 125 Summer Street, Boston, MA 02110–1618 (US).

(54) Title: APPARATUS AND METHOD FOR DISTRIBUTING AUTHENTICATION KEYS TO NETWORK DEVICES IN A MULTICAST

(57) Abstract

An apparatus and method of distributing an authentication key to multicast network devices in a multicast loads a set of the multicast network devices with a security key that is unavailable to network devices that are not members of the multicast. The authentication key then is encrypted via the security key to produce an encrypted authentication key that is forwarded to the set of multicast network devices. The security key enables the set of multicast network devices to decrypt the encrypted authentication key to produce the authentication key. The authentication key preferably is utilized by the multicast network devices to authenticate messages transmitted in the multicast.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

APPARATUS AND METHOD FOR DISTRIBUTING AUTHENTICATION KEYS TO NETWORK DEVICES IN A MULTICAST

FIELD OF THE INVENTION

The invention generally relates networks and, more particularly, the invention relates to multicast transmissions across a computer network.

BACKGROUND OF THE INVENTION

Multicasting is a well known method of transmitting messages to selected groups of users across a network, such as the Internet. One simple example of multicasting entails transmitting an E-mail message to a plurality of users that each are on a mailing list. Video conferencing and teleconferencing also use multicasting principles and thus, often are referred to as "multiconferencing." Many of the messages transmitted during a multicast include multicast control parameters that control the execution of the multicast ("control messages"). One exemplary type of control message enables nodes to join an ongoing multicast.

Problems arise when an unauthorized network device transmits a control message to a multicast session. For example, an unauthorized network device undesirably may transmit a control message that prematurely ends a multicast session. One solution to this problem (recently proposed by the PIM Working Group of the Internet Engineering Task Force) utilizes well known key encryption techniques to authenticate control messages transmitted between routers. To that end, a symmetrical authentication key is provided to each router in the multicast to encrypt and decrypt control messages transmitted in the multicast. Accordingly, upon receipt of a control message from another router, a receiving router can confirm that the control message was transmitted from an authorized router in the multicast by decrypting the received control message with the symmetrical authentication key. This method is expected to provide satisfactory results as long as the symmetrical authentication key is not ascertained by routers or other network devices that are not authorized to participate in the multicast. To date, however, this proposed solution does not address the problem of securely and efficiently disseminating the symmetrical authentication key to the authorized network devices in the multicast.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, an apparatus and method of distributing an authentication key to multicast network devices in a multicast loads a set of the multicast network devices with a security key that is unavailable to network devices that are not members of the multicast. The authentication key then is encrypted via the security key to produce an encrypted authentication key that is forwarded to the set of multicast network devices. The security key enables the set of multicast network devices to decrypt the encrypted authentication key to produce the authentication key. The authentication key preferably is utilized by the multicast network devices to authenticate messages transmitted in the multicast.

In preferred embodiments, the security key, which may be manually loaded into memory of each multicast network device, is an asymmetrical key pair. In other embodiments, the security key is a symmetrical key. The multicast may be configured in accord with any known multicast protocol, including the protocol independent multicast protocol. When configured as such, the authentication key may be produced by a rendezvous point multicast network device in the multicast.

In alternative embodiments, the authentication key is changed during the multicast to produce a modified key. Accordingly, in such circumstances, the modified key is encrypted with the security key to produce an encrypted modified key that is forwarded to each multicast network device. In other embodiments, the encrypted authentication key is forwarded by a forwarding multicast network device, where the security key is selected to authenticate the identity of the forwarding multicast network device. The security key also may be selected to ensure the secrecy of the encrypted authentication key.

The network devices may be routers or other network devices. The set of multicast network devices may include all of the multicast network devices that are members of the multicast. For example, the set of multicast network devices may be a set of routers executing the protocol independent multicast protocol.

In accordance with another aspect of the invention, an apparatus and method of distributing an authentication key to network devices in a multicast encrypts the authentication key with a security key to produce an encrypted authentication key. The

secret key is unavailable to network devices that are not members of the multicast, and available to network devices that are members of the multicast. The encrypted authentication key then is forwarded to the multicast network devices so that each such multicast network device can decrypt the encrypted authentication key with the security key to produce the authentication key.

In preferred embodiments of this aspect, the security key, which may be manually loaded into memory of each multicast network device, is an asymmetrical key pair. In other embodiments, the security key is a symmetrical key. The multicast may be configured in accord with any known multicast protocol, including the protocol independent multicast protocol. When configured as such, the authentication key may be produced by a rendezvous point multicast network device in the multicast.

In alternative embodiments of this aspect, the authentication key is changed during the multicast to produce a modified key. Accordingly, in such circumstances, the modified key is encrypted with the security key to produce an encrypted modified key that is forwarded to each multicast network device. In other embodiments, the encrypted authentication key is forwarded by a forwarding multicast network device, where the security key is selected to authenticate the identity of the forwarding multicast network device. The security key also may be selected to ensure the secrecy of the encrypted authentication key.

In accordance with other aspects of the invention, an apparatus and method of distributing an authentication key to multicast network devices in a multicast first receives an encrypted authentication key that is an encrypted form of the authentication key. The encrypted form preferably is encrypted by a secret key. The secret key then is utilized to decrypt the encrypted authentication key to produce the authentication key. The security key is unavailable to network devices that are not members of the multicast.

In preferred embodiments of this aspect, the security key is loaded into each network device in the multicast. The security key may be an asymmetrical key pair, or a symmetrical key. The multicast preferably is configured in accord with the protocol independent multicast network protocol.

In accordance with yet another aspect of the invention, an apparatus and method of distributing an authentication key to multicast network devices in a multicast loads each of

the multicast network devices with a security key that is unavailable to network devices that are not members of the multicast. The authentication key then is encrypted via the security key to produce an encrypted authentication key that is forwarded to the set of multicast nctwork devices. Each multicast network device then is controlled to utilize the secret key to decrypt the encrypted authentication key, thus producing the authentication key.

Preferred embodiments of the invention are implemented as a computer program product having a computer usable medium with computer readable program code thereon. The computer readable code may be read and utilized by the computer system in accordance with conventional processes.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects and advantages of the invention will be appreciated more fully from the following further description thereof with reference to the accompanying drawings wherein:

Figure 1 schematically shows an exemplary network arrangement in which preferred embodiments of the invention may be implemented.

Figure 2A schematically show a key distribution router that may be configured in accord with preferred embodiments of the invention.

Figure 2B schematically show a protocol independent multicast router that may be configured in accord with preferred embodiments of the invention.

Figure 3 shows a preferred process for initiating a protocol independent multicast in the network shown in figure 1.

Figure 4 shows a preferred process for distributing keys to protocol independent multicast routers.

DESCRIPTION OF PREFERRED EMBODIMENTS

Preferred embodiments of the invention relate to the secure distribution of an authentication key that confirms the authenticity of messages transmitted in a multicast ("multicast messages"). More particularly, the authentication key is utilized by multicast network devices to authenticate multicast messages, thereby ensuring that multicast

messages received by multicast network devices were produced by network devices that are authorized to participate in the multicast. As discussed in greater detail below, the authentication key is distributed in an encrypted form within a key dissemination message that receiving network devices can decrypt by means of an asymmetrical security key. The security key is not available to network devices that are not authorized to participate in the multicast, thus ensuring both the authenticity and secrecy of key dissemination messages that distribute the authentication key to the multicast network devices.

Figure 1 schematically shows an exemplary multicast network 100 in which preferred embodiments of the invention may be implemented. The network 100 preferably is executing in accord with a known multicast protocol, such as the protocol independent multicast protocol ("PIM protocol"). It should be noted, however, that although preferred embodiments are discussed in terms of the PIM protocol, principles of the invention may be applied to other multicast protocols, such as the Internet Protocol multicast protocol ("IP Multicast"). The PIM protocol therefore is discussed for exemplary purposes only and is not intended to limit the scope of the invention.

The multicast network 100 includes a rendezvous point router 102 for distributing multicast parameters and forming the multicast distribution tree, a bootstrap router 104 for selecting and identifying the rendezvous point router 102, a plurality of PIM routers 106 that operate in accord with the PIM network protocol, and one or more non-PIM routers 108 that merely forward PIM multicast messages toward the PIM routers 106. In addition, the network 100 also includes a key distribution router 110 for generating and transmitting encryption keys for use in the multicast. Each of the network devices of the multicast network 100 preferably communicates across a large scale network, such as the Internet.

Figure 2A schematically shows several internal components of the key distribution router 110. In particular, the key distribution router 110 includes a key generator 200 for generating encryption keys in accord with preferred embodiments of the invention, an encrypter 202 for producing key dissemination messages, and a transmitter 204 for transmitting messages to multicast groups. The cooperation and configuration of these internal components is discussed in greater detail below with reference to figures 3 and 4.

Figure 2B schematically shows several internal components of a PIM router 106 that may be utilized in the multicast network 100 shown in figure 1. In particular, the PIM

router 106 includes a receiver 206 for receiving messages from other nodes of the multicast, a decrypter 208 for decrypting key dissemination messages in accord with preferred embodiments of the invention, memory 210 for storing data (*e.g.*, the security key preloaded into the PIM router 106), and control logic 212 for executing PIM functionality, such as decrypting (*i.e.*, authenticating) multicast messages with the authentication key. In a manner similar to the key distribution router 110 shown in figure 2A, the cooperation and configuration of these internal components is discussed in greater detail below with reference to figures 3 and 4.

Figure 3 shows a preferred process of initiating a multicast utilizing the PIM protocol. The process begins at step 300, in which various keys utilized in the multicast are distributed to the PIM routers 106. Among those keys are a bootstrap router asymmetrical public key pair ("bootstrap key") and a rendezvous key, both of which are known in the art. The bootstrap key, which preferably is a public key pair that complies with the well known "Rivest, Shamir, and Adleman cryptography method" (RSA cryptography method), is used to encrypt a message identifying the rendezvous point router 102. The rendezvous key preferably is a symmetrical key that is utilized for communication between the rendezvous point router 102 and the bootstrap router 104.

In accord with preferred embodiments of the invention, the prior noted security key also is distributed to each PIM router 106. The security key preferably is a key pair having a "semi-public" key and a secret key. The semi-public key is not considered to be a public key since it is not available from a publicly available certification authority. Accordingly, the semi-public key is loaded into the memory 210 of each PIM router 106 that is to participate in the multicast shown in figure 1. For example, the semi-public key may be preloaded during manufacture of a given PIM router 106, or may be manually loaded via a portable medium, such as a CD-ROM or floppy disk. Accordingly, the semi-public key is not available to network devices other than those loaded with the semi-public key.

Step 300 further includes the distribution of the authentication key to each selected PIM router 106. Details of the distribution of the authentication key and other keys are discussed below with regard to the process shown in figure 4.

Once the keys are distributed, the process continues to step 302, in which the bootstrap router 104 first selects the PIM router 106 that is to act as the rendezvous point

router 102, and then broadcasts the identity of the selected rendezvous point router 102 to the PIM routers 106 in the multicast. To that end, the bootstrap router 104 conducts a well known election process to select the rendezvous point router 102. The identity of the selected rendezvous point router 102 then is encrypted (*i.e.*, authenticated or digitally signed) via the bootstrap secret key, and transmitted to the multicast network 100. Upon receipt, the receiving PIM routers 106 decrypt (*i.e.*, authenticate) the encrypted identity of the rendezvous point router 102 by means of the bootstrap public key. Encrypting and decrypting (*i.e.*, authenticating) the rendezvous point router identity in this manner ensures that its transmission is from a bootstrap router 104 that is authorized to initiate the multicast.

The process then continues to step 304, in which the router tables in the PIM routers 106 are updated accordingly, and other multicast parameters are set in accord with conventional processes, thus ending the process. Once this process is complete, the multicast is initiated and the PIM routers 106 may transmit multicast messages across the multicast network 100 in accord with conventional processes.

Figure 4 shows a preferred process for distributing keys (*i.e.*, particularly the authentication key) to protocol independent multicast routers as discussed above in step 300. The process begins at step 400, in which the key distribution router 110 generates the bootstrap key and the rendezvous key. Once generated, the key distribution router 110 transmits both the bootstrap and rendezvous keys to the bootstrap router 104, and the rendezvous key to the rendezvous point router 102 (step 402). To that end, a secure channel is established between the key distribution router 110 and each of the bootstrap router 104 and the rendezvous point router 102 for transmitting such keys. The key distribution router 110 then may utilize the secret key of the security key to encrypt the public key portion of the bootstrap key. The resulting encrypted bootstrap key then may be transmitted by the key distribution router 110 to each of the PIM routers 106 participating in the multicast (step 404).

The authentication key then is generated by the key distribution router 110 (step 406), and then encrypted with the secret key of the security key by the key distribution router encrypter 202 (step 408). As noted above, the authentication key preferably is encrypted by means of a cryptographic algorithm (*e.g.*, the RSA cryptography method or

the Data Encryption Standard) that produces the resultant key dissemination message. In such case, the hash may be appended to a message. The process continues to step 410, in which the encrypted authentication key is transmitted to the respective PIM routers 106. This transmission may be made in any conventional manner, such as via a unicast or via the distribution tree.

Upon receipt by a given PIM router 106 in the multicast, the encrypted authentication message is decrypted by means of the semi-public key of the security key (step 412). Multicast messages then may be freely transmitted between the PIM routers 106 within the multicast domain. As noted above, multicast messages received by non-PIM routers 108 are merely re-transmitted in their entireties toward PIM routers 106 in the multicast.

In preferred embodiments, the authentication key is periodically changed to ensure that an unauthorized network device monitoring multicast traffic cannot determine its identity. Accordingly, the key distribution router 110 periodically changes the authentication key by transmitting a message to the PIM routers 106 indicating that such message includes a new authentication key. A new key may be generated every several minutes, hours, days, or other selected time interval. In some embodiments, no time interval is selected and thus, the authentication key is sporadically changed. Accordingly, the process continues to step 414, in which the key distribution router 110 determines if the authentication key is to be changed. If it is not to be changed, then the process ends. If it is changed, then the process loops to step 406, in which the key distribution router 110 generates a new authentication key.

Accordingly, as noted above, restricting the identity of the semi-public key to those network devices in the multicast domain ensures that both the authentication key received by the PIM routers 106 is from an authorized member of the multicast domain (*i.e.*, the key distribution router 110), and that its identity cannot be ascertained by an unauthorized network device (*i.e.*, a network device that is not an authorized member of the multicast) intercepting the encrypted authentication key after it is transmitted by the key distribution router 110. A network device thus cannot participate in the discussed multicast if it does not have a copy of the semi-public key in its memory 210.

In alternative embodiments, the security key is a symmetrical key. It should be noted that the order of various steps of the processes shown in figures 3 and 4 may be varied as necessary without affecting the execution of the process. It also should be noted that the network devices utilized in the multicast network 100 may be any network device and thus, are not intended to be limited to routers. Routers are discussed for exemplary purposes only and should not be construed to limit the use or scope of preferred embodiments of the invention.

Preferred embodiments of the invention may be implemented in any conventional computer programming language. For example, preferred embodiments may be implemented in a procedural programming language (*e.g.*, "C") or an object oriented programming language (*e.g.*, "C++"). Alternative embodiments of the invention may be implemented as preprogrammed hardware elements (*e.g.*, application specific integrated circuits), or other related components.

Alternative embodiments of the invention may be implemented as a computer program product for use with a computer system. Such implementation may include a series of computer instructions fixed either on a tangible medium, such as a computer readable media (*e.g.*, a diskette, CD-ROM, ROM, or fixed disk), or transmittable to a computer system via a modem or other interface device, such as a communications adapter connected to a network over a medium. The medium may be either a tangible medium (*e.g.*, optical or analog communications lines) or a medium implemented with wireless techniques (*e.g.*, microwave, infrared or other transmission techniques). The series of computer instructions preferably embodies all or part of the functionality previously described herein with respect to the system. Those skilled in the art should appreciate that such computer instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Furthermore, such instructions may be stored in any memory device, such as semiconductor, magnetic, optical or other memory devices, and may be transmitted using any communications technology, such as optical, infrared, microwave, or other transmission technologies. It is expected that such a computer program product may be distributed as a removable medium with accompanying printed or electronic documentation (*e.g.*, shrink wrapped software), preloaded with a

computer system (*e.g.*, on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the network (*e.g.*, the Internet or World Wide Web).

Although various exemplary embodiments of the invention have been disclosed, it should be apparent to those skilled in the art that various changes and modifications can be made which will achieve some of the advantages of the invention without departing from the true scope of the
invention. These and other obvious modifications are intended to be covered by the appended claims.

I claim:

1. A method of distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the method comprising:

loading a security key into a set of the multicast network devices, the security key being unavailable to network devices that are not members of the multicast;

encrypting the authentication key with the security key to produce an encrypted authentication key; and

forwarding the encrypted authentication key to the set of the multicast network devices,

the security key enabling the set of the multicast network devices to decrypt the encrypted authentication key to produce the authentication key.

2. The method as defined by claim 1 wherein the security key is an asymmetrical key pair.

3. The method as defined by claim 1 wherein the security key is a symmetrical key.

4. The method as defined by claim 1 wherein each network device includes a memory, the step of loading comprising:

manually entering the security key into the memory of each multicast network device.

5. The method as defined by claim 1 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

6. The method as defined by claim 5 wherein the authentication key is produced by a rendezvous point multicast network device in the multicast.

7. The method as defined by claim 1 wherein the authentication key is changed during the multicast.

8. The method as defined by claim 1 further comprising:

changing the authentication key during the multicast to produce a modified key;

encrypting the modified key with the security key to produce an encrypted modified key; and

forwarding the encrypted modified key to each multicast network device.

9. The method as defined by claim 1 wherein the encrypted authentication key is forwarded by a forwarding multicast network device, the security key being selected to authenticate the identity of the forwarding multicast network device.

10. The method as defined by claim 9 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

11. The method as defined by claim 1 wherein the network devices are routers.

12. The method as defined by claim 1 wherein the set of multicast network devices includes all of the multicast network devices that are members of the multicast.

13. An apparatus for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the apparatus comprising:

a key loader that loads a security key into a set of the multicast network devices, the security key being unavailable to network devices that are not members of the multicast;

an encrypter that encrypts the authentication key with the security key to produce an encrypted authentication key; and

a transmitter that forwards the encrypted authentication key to the set of the multicast network devices,

the security key enabling the set of multicast network devices to decrypt the encrypted authentication key to produce the authentication key.

14. The apparatus as defined by claim 13 wherein the security key is an asymmetrical key pair.

15. The apparatus as defined by claim 13 wherein the security key is a symmetrical key.

16. The apparatus as defined by claim 13 wherein each network device includes a memory, the key loader comprising means for manually storing the security key into the memory of each multicast network device.

17. The apparatus as defined by claim 13 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

18. The apparatus as defined by claim 17 wherein the authentication key is produced by a rendezvous point multicast network device in the multicast.

19. The apparatus as defined by claim 13 wherein the authentication key is changed during the multicast.

20. The apparatus as defined by claim 13 further comprising:

a key changer that changes the authentication key during the multicast to produce a modified key;

the encrypter encrypting the modified key with the security key to produce an encrypted modified key, the transmitter forwarding the encrypted modified key to each multicast network device.

21. The apparatus as defined by claim 13 wherein the encrypted authentication key is forwarded by a forwarding multicast network device, the security key being selected to authenticate the identity of the forwarding multicast network device.

22. The apparatus as defined by claim 21 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

23. The apparatus as defined by claim 13 wherein the network devices are routers.

24. The apparatus as defined by claim 13 wherein the set of multicast network devices includes all of the multicast network devices that are members of the multicast.

25. A computer program product for use on a computer system for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the computer program product comprising a computer usable medium having computer readable program code thereon, the computer readable program code including:

program code for loading a security key into a set of the multicast network devices, the security key being unavailable to network devices that are not members of the multicast;

program code for encrypting the authentication key with the security key to produce an encrypted authentication key; and

program code for forwarding the encrypted authentication key to the set of the multicast network devices,

the security key enabling the set of the multicast network devices to decrypt the encrypted authentication key to produce the authentication key.

26. The computer program product as defined by claim 25 wherein the security key is an asymmetrical key pair.

27. The computer program product as defined by claim 25 wherein the security key is a symmetrical key.

28. The computer program product as defined by claim 25 wherein each network device includes a memory, the program code for loading comprising:

program code for manually entering the security key into the memory of each multicast network device.

29. The computer program product as defined by claim 25 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

30. The computer program product as defined by claim 29 wherein the authentication key is produced by a rendezvous point multicast network device in the multicast.

31. The computer program product as defined by claim 25 wherein the authentication key is changed during the multicast.

32. The computer program product as defined by claim 25 further comprising:

program code for changing the authentication key during the multicast to produce a modified key;

program code for encrypting the modified key with the security key to produce an encrypted modified key; and

program code for forwarding the encrypted modified key to each multicast network device.

33. The computer program product as defined by claim 25 wherein the encrypted authentication key is forwarded by a forwarding multicast network device, the security key being selected to authenticate the identity of the forwarding multicast network device.

34. The computer program product as defined by claim 33 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

35. The computer program product as defined by claim 25 wherein the network devices are routers.

36. The computer program product as defined by claim 25 wherein the set of multicast network devices includes all of the multicast network devices that are members of the multicast.

37. A method of distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the method comprising:

encrypting the authentication key with a security key to produce an encrypted authentication key, the security key being unavailable to network devices that are not members of the multicast, the security key being available to the multicast network devices; and

forwarding the encrypted authentication key to the multicast network devices so that each multicast network device can decrypt the encrypted authentication key with the security key to produce the authentication key.

38. The method as defined by claim 37 wherein the security key is an asymmetrical key pair.

39. The method as defined by claim 37 wherein the security key is a symmetrical key.

40. The method as defined by claim 37 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

41. The method as defined by claim 40 wherein the authentication key is produced by a rendezvous point network device in the multicast.

42. The method as defined by claim 37 wherein the authentication key is changed during the multicast.

43. The method as defined by claim 37 further comprising:

changing the authentication key during the multicast to produce a modified key;

encrypting the modified key with the security key to produce an encrypted modified key; and

forwarding the encrypted modified key to each network device.

44. The method as defined by claim 37 wherein the encrypted authentication key is forwarded by a forwarding network device, the security key being selected to authenticate the identity of the forwarding network device.

45. The method as defined by claim 44 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

46. The method as defined by claim 37 wherein the network devices are routers.

47. An apparatus of distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the apparatus comprising:

an encrypter that encrypts the authentication key with a security key to produce an encrypted authentication key, the security key being unavailable to network devices that are not members of the multicast, the security key being available to the multicast network devices; and

a transmitter that forwards the encrypted authentication key to the multicast network devices so that each multicast network device can decrypt the encrypted authentication key with the security key to produce the authentication key.

48. The apparatus as defined by claim 47 wherein the security key is an asymmetrical key pair.

49. The apparatus as defined by claim 47 wherein the security key is a symmetrical key.

50. The apparatus as defined by claim 47 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

51. The apparatus as defined by claim 50 wherein the authentication key is produced by a rendezvous point network device in the multicast.

52. The apparatus as defined by claim 47 wherein the authentication key is changed during the multicast.

53. The apparatus as defined by claim 47 further comprising:

a key changer that changes the authentication key during the multicast to produce a modified key,

the encrypter encrypting the modified key with the security key to produce an encrypted modified key, the transmitter forwarding the encrypted modified key to each network device.

54. The apparatus as defined by claim 47 wherein the encrypted authentication key is forwarded by a forwarding network device, the security key being selected to authenticate the identity of the forwarding network device.

55. The apparatus as defined by claim 54 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

56. The apparatus as defined by claim 47 wherein the network devices are routers.

57. A computer program product for use on a computer system for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast,, the computer program product comprising a computer usable medium having computer readable program code thereon, the computer readable program code including:

program code for encrypting the authentication key with a security key to produce an encrypted authentication key, the security key being unavailable to network devices that are not members of the multicast, the security key being available to the multicast network devices; and

program code for forwarding the encrypted authentication key to the multicast network devices so that each multicast network device can decrypt the encrypted authentication key with the security key to produce the authentication key.

58. The computer program product as defined by claim 57 wherein the security key is an asymmetrical key pair.

59. The computer program product as defined by claim 57 wherein the security key is a symmetrical key.

60. The computer program product as defined by claim 57 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

61. The computer program product as defined by claim 60 wherein the authentication key is produced by a rendezvous point network device in the multicast.

62. The computer program product as defined by claim 57 wherein the authentication key is changed during the multicast.

63. The computer program product as defined by claim 57 further comprising:

program code for changing the authentication key during the multicast to produce a modified key;

program code for encrypting the modified key with the security key to produce an encrypted modified key; and

program code for forwarding the encrypted modified key to each network device.

64. The computer program product as defined by claim 57 wherein the encrypted authentication key is forwarded by a forwarding network device, the security key being selected to authenticate the identity of the forwarding network device.

65. The computer program product as defined by claim 64 wherein the security key is selected to ensure the secrecy of the encrypted authentication key.

66. The computer program product as defined by claim 57 wherein the network devices are routers.

67. A method of distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the method comprising:

receiving an encrypted authentication key, the encrypted authentication key being the authentication key encrypted by a security key; and

utilizing the security key to decrypt the encrypted authentication key to produce the authentication key, the security key being unavailable to network devices that are not members of the multicast.

68. The method as defined by claim 67 further comprising:

loading the security key into each network device in the multicast.

69. The method as defined by claim 67 wherein the security key is an asymmetrical key pair.

70. The method as defined by claim 67 wherein the security key is a symmetrical key.

71. The method as defined by claim 67 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

72. The method as defined by claim 71 wherein the authentication key is produced by a rendezvous point network device in the multicast.

73. The method as defined by claim 67 further comprising:

receiving an encrypted modified key, the encrypted modified key being a new authentication key that is encrypted by the security key; and

utilizing the security key to decrypt the encrypted modified key to produce the new authentication key.

74. The method as defined by claim 67 wherein the network devices are routers.

75. An apparatus for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the apparatus comprising:

a receiver that receives an encrypted authentication key, the encrypted authentication key being the authentication key encrypted by a security key; and

a decrypter that utilizes the security key to decrypt the encrypted authentication key to produce the authentication key, the security key being unavailable to network devices that are not members of the multicast.

76. The apparatus as defined by claim 75 further comprising:

a key loader that loads the security key into each network device in the multicast.

77. The apparatus as defined by claim 75 wherein the security key is an asymmetrical key pair.

78. The apparatus as defined by claim 75 wherein the security key is a symmetrical key.

79. The apparatus as defined by claim 75 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

80. The apparatus as defined by claim 79 wherein the authentication key is produced by a rendezvous point network device in the multicast.

81. The apparatus as defined by claim 75 wherein the receiver receives an encrypted modified key, the encrypted modified key being a new authentication key that is encrypted by the security key; and

the decrypter utilizing the security key to decrypt the encrypted modified key to produce the new authentication key.

82. The apparatus as defined by claim 75 wherein the network devices are routers.

83. A computer program product for use on a computer system for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the computer program product comprising a computer usable medium having computer readable program code thereon, the computer readable program code including:

program code for receiving an encrypted authentication key, the encrypted authentication key being the authentication key encrypted by a security key; and

program code for utilizing the security key to decrypt the encrypted authentication key to produce the authentication key, the security key being unavailable to network devices that are not members of the multicast.

84. The computer program product as defined by claim 83 further comprising:

program code for loading the security key into each network device in the multicast.

85. The computer program product as defined by claim 83 wherein the security key is an asymmetrical key pair.

86. The computer program product as defined by claim 83 wherein the security key is a symmetrical key.

87. The computer program product as defined by claim 83 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

88. The computer program product as defined by claim 87 wherein the authentication key is produced by a rendezvous point network device in the multicast.

89. The computer program product as defined by claim 83 further comprising:

program code for receiving an encrypted modified key, the encrypted modified key being a new authentication key that is encrypted by the security key; and

program code for utilizing the security key to decrypt the encrypted modified key to produce the new authentication key.

90. The computer program product as defined by claim 83 wherein the network devices are routers.

91. A method of distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the method comprising:

loading a security key into each of the multicast network devices, the security key being unavailable to network devices that are not members of the multicast;

encrypting the authentication key with the security key to produce an encrypted authentication key; and

forwarding the encrypted authentication key to each multicast network device; and

controlling each multicast network device to decrypt the encrypted authentication key to produce the authentication key, each multicast network device utilizing the secret key to decrypt the encrypted authentication key.

92. The method as defined by claim 91 wherein the security key is an asymmetrical key pair.

93. The method as defined by claim 91 wherein the security key is a symmetrical key.

94. The method as defined by claim 91 wherein each multicast network device includes a memory, the step of loading comprising:

manually entering the security key into the memory of each multicast network device.

95. The method as defined by claim 91 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

96. The method as defined by claim 91 further comprising:

changing the authentication key during the multicast to produce a modified key;

encrypting the modified key with the security key to produce an encrypted modified key; and

forwarding the encrypted modified key to each multicast network device.

97. A system for distributing an authentication key to multicast network devices in a multicast, the authentication key being utilized by the multicast network devices to authenticate messages transmitted in the multicast, the system comprising:

an input that loads a security key into each of the multicast network devices, the security key being unavailable to network devices that are not members of the multicast;

an encrypter that encrypts the authentication key with the security key to produce an encrypted authentication key; and

an output that forwards the encrypted authentication key to each multicast network device; and

each multicast network device having a decrypter that decrypts the encrypted authentication key to produce the authentication key, each decrypter utilizing the secret key to decrypt the encrypted authentication key.

98. The system as defined by claim 97 wherein the security key is an asymmetrical key pair.

99. The system as defined by claim 97 wherein the security key is a symmetrical key.

100. The system as defined by claim 97 wherein each multicast network device includes a memory, the input including means for manually entering the security key into the memory of each multicast network device.

101. The system as defined by claim 97 wherein the multicast is configured in accord with the protocol independent multicast network protocol.

102. The system as defined by claim 97 further comprising:

a key changer that changes the authentication key during the multicast to produce a modified key,

the encrypter encrypting the modified key with the security key to produce an encrypted modified key, the output forwarding the encrypted modified key to each multicast network device.

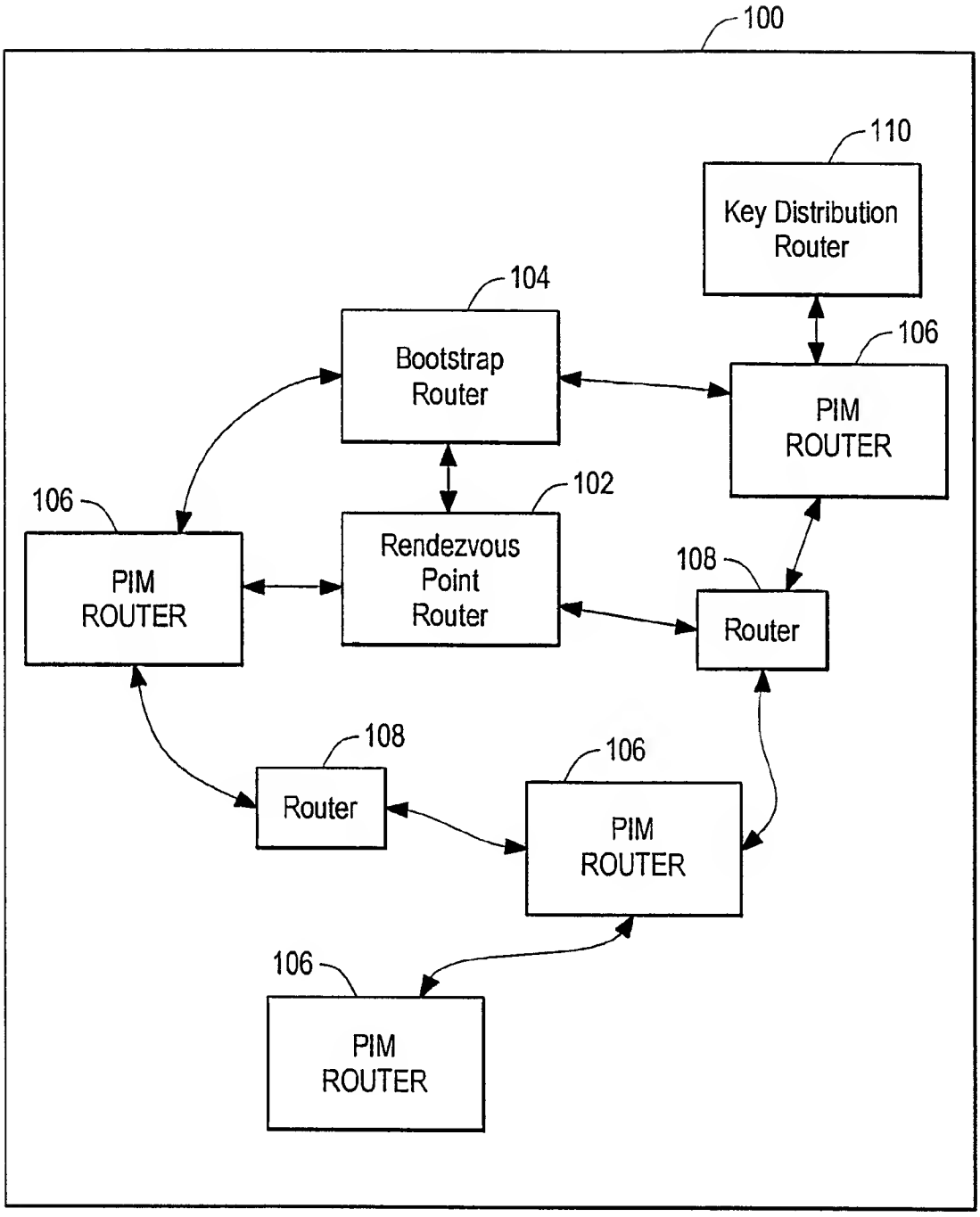

100
110
Key Distribution Router
104
Bootstrap Router
106
PIM ROUTER
106
PIM ROUTER
102
Rendezvous Point Router
108
Router
108
Router
106
PIM ROUTER
106
PIM ROUTER

FIG. 1

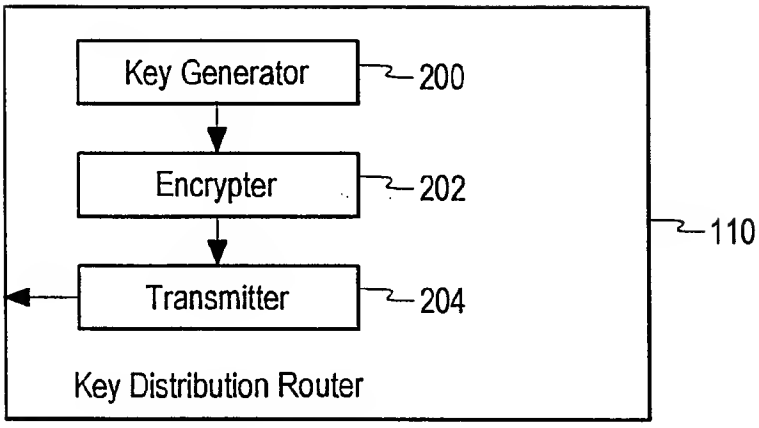

Key Generator
200
Encrypter
202
Transmitter
204
110
Key Distribution Router

FIG. 2A

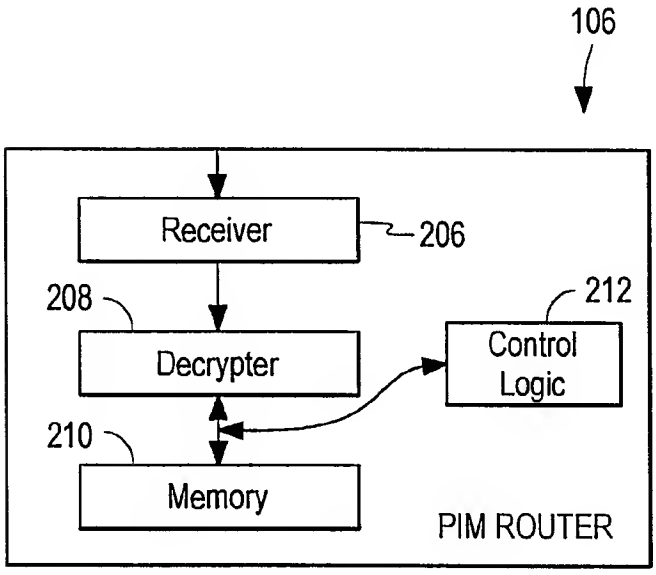

106
Receiver
206
208
212
Decrypter
Control Logic
210
Memory
PIM ROUTER

FIG. 2B

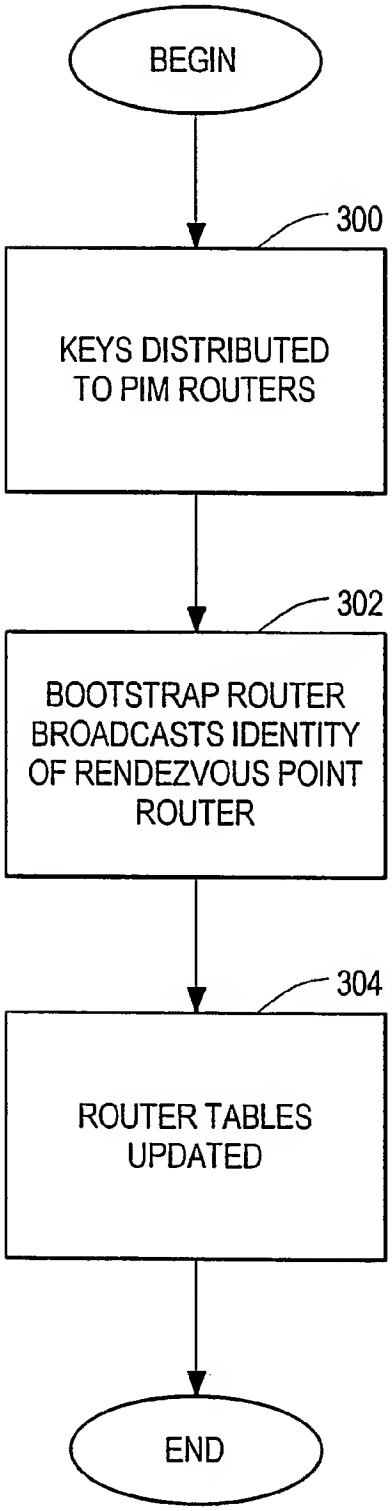

BEGIN
300
KEYS DISTRIBUTED TO PIM ROUTERS
302
BOOTSTRAP ROUTER BROADCASTS IDENTITY OF RENDEZVOUS POINT ROUTER
304
ROUTER TABLES UPDATED
END

FIG. 3

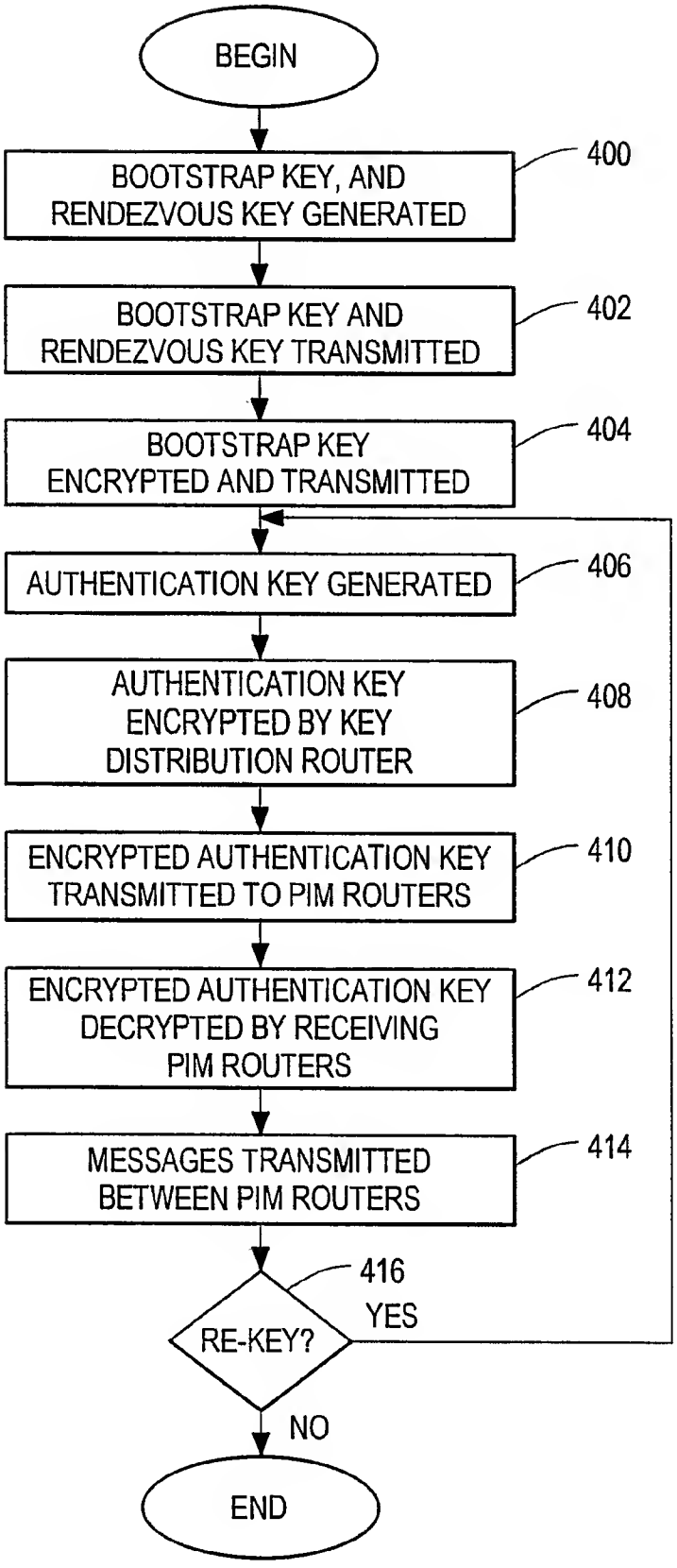

BEGIN
BOOTSTRAP KEY, AND RENDEZVOUS KEY GENERATED
400
BOOTSTRAP KEY AND RENDEZVOUS KEY TRANSMITTED
402
BOOTSTRAP KEY ENCRYPTED AND TRANSMITTED
404
AUTHENTICATION KEY GENERATED
406
AUTHENTICATION KEY ENCRYPTED BY KEY DISTRIBUTION ROUTER
408
ENCRYPTED AUTHENTICATION KEY TRANSMITTED TO PIM ROUTERS
410
ENCRYPTED AUTHENTICATION KEY DECRYPTED BY RECEIVING PIM ROUTERS
412
MESSAGES TRANSMITTED BETWEEN PIM ROUTERS
414
416
RE-KEY?
YES
NO
END

FIG. 4